State of Michigan (agency name)
Evaluation of the Internal Control Structure - Application Controls
As of September 30, 20___

Purpose: Departments should use this tool to assist in evaluating information technology (IT) application controls for applications or systems in which the department is the business owner.

Background: The Michigan Department of Information Technology (MDIT) is responsible for assessing the State's general information technology (IT) controls. General IT controls relate to activities that provide for the proper operation of application systems. General controls encompass, strategic planning, business continuity, contingency planning, system development methodology, procedures for documenting, reviewing, testing and approving system changes, and a variety of other control activities.

Departments, as application business owners, are responsible for establishing, maintaining, and monitoring internal controls over specific applications and the environment in which they operate.

Application Specific Controls consist of mechanisms in place over each separate computer system that helps to ensure authorized data is processed completely, accurately, and reliably. Controls may relate to data origin; input, processing, output, and application access controls; audit trails; and documentation.

Application Environment Controls apply to the entire environment in which an application resides, rather than to an individual application. . Application environment controls may include controls related to service level agreements, data storage and backup, data management, and other areas.

(1)	(2)	(3)				(4)			(5)	(6)
Optimal Internal Controls	Agency, Division/Office and Staff (Non-DIT) Responsible for IT Process and Related Controls identify the activity and business owner responsible for each IT process (e.g., agency, division, office and/or staff)	Internal Control Existence (a)				Performance Effectiveness			Description/Comments (this column must be completed) description of controls, activities, formal policies, procedures, and practices that represent internal controls related to the IT process and whether alternative or compensating controls and plans and time frames exist for addressing deficiencies	Monitoring (this column must be completed) description of activities performed to ensure controls in place are working
		Documented	Not Documented	No Control in Place	Not Applicable (b)	Satisfactory	Ineffective/Inefficient	Not Applicable		
Risk Category: Security Control Issues										
Description/Purpose: to evaluate controls over access to data, application documentation, and information transfer by implementing and monitoring controls regarding user identifies, physical security, encryption and other means.										
COBIT Reference: DS-5										
Does management establish and enforce user identities and access rights for the application?										
Has management established a process for issuing, maintaining, and removing user access rights?										
Does management regularly test and monitor security over the application?										
Has management defined possible security incidents/policy violations?										
Has management secured logical and physical security over application documentation (i.e. access restrictions/non-disclosure)?										
Has management established a process to manage the transforming of sensitive information into unreadable/identifiable information and its reverse process in the application?										
Has management established a process to protect the application from viruses, worms, Trojans, logic bombs, spyware, etc. through updated security patches, virus protection software, etc.?										

(a) When possible, obtain applicable documentation and/or flowcharts for your future needs/requirements. (b) Please explain in the Description/Comments Column

(1)	(2)	(3)				(4)			(5)	(6)
Optimal Internal Controls	Agency, Division/Office and Staff (Non-DIT) Responsible for IT Process and Related Controls identify the activity and business owner responsible for each IT process (e.g., agency, division, office and/or staff)	Internal Control Existence (a)				Performance Effectiveness			Description/Comments (this column must be completed) description of controls, activities, formal policies, procedures, and practices that represent internal controls related to the IT process and whether alternative or compensating controls and plans and time frames exist for addressing deficiencies	Monitoring (this column must be completed) description of activities performed to ensure controls in place are working
		Documented	Not Documented	No Control in Place	Not Applicable (b)	Satisfactory	Ineffective/Inefficient	Not Applicable		
Are sensitive data associated with the application only exchanged over secure paths?										

Conclusion for this Section (Include All Weaknesses Identified)

Risk Category: Risk Assessment and Management Controls										
Description/Purpose: to evaluate the risk assessment framework that enables management to use a structured process to identify, analyze, communicate, and respond to risks and impacts on data, information, applications, systems and their controls.										
COBIT Reference: PO-9										
Has management defined or approved risk evaluation criteria for the application?										
Does management assess the risks associated with the application for their likelihood and impact?										
Has management mitigated the identified application risks through avoidance, reduction, sharing, acceptance, or a combination of these options to an acceptable level?										
Does management maintain and monitor its efforts to mitigate the identified application risks?										

Conclusion for this Section (Include All Weaknesses Identified)

Risk Category: Access Controls										
Description/Purpose: to evaluate the protection of computer assets and data through physical security measures, environmental controls, and access controls by adequately managing facilities and implementing physical security.										
COBIT Reference: DS-12										
Has management established or approved physical security measures defining the security perimeter, authorized access, security zones, location of critical equipment, shipping and receiving areas related to the application?										
Is physical security access for the application defined and limited to business needs?										
Is the application and equipment that houses the application physically protected with smoke detectors, raised floors, water sensors, etc. from environmental factors like smoke/fire, water damage, static electricity, food, etc.?										

(a) When possible, obtain applicable documentation and/or flowcharts for your future needs/requirements.

(b) Please explain in the Description/Comments column.

(1)	(2)	(3)				(4)			(5)	(6)
Optimal Internal Controls	Agency, Division/Office and Staff (Non-DIT) Responsible for IT Process and Related Controls identify the activity and business owner responsible for each IT process (e.g., agency, division, office and/or staff)	Internal Control Existence (a)				Performance Effectiveness			Description/Comments (this column must be completed) description of controls, activities, formal policies, procedures, and practices that represent internal controls related to the IT process and whether alternative or compensating controls and plans and time frames exist for addressing deficiencies	Monitoring (this column must be completed) description of activities performed to ensure controls in place are working
		Documented	Not Documented	No Control in Place	Not Applicable (b)	Satisfactory	Ineffective/Inefficient	Not Applicable		

Conclusion for this Section (Include All Weaknesses Identified)

Risk Category: Change Control, Analysis, and Management										
Description/Purpose: to evaluate the controls over changes to applications through management's procedures, assessment/analysis, and tracking of changes.										
COBIT Reference: AI-6										
Has a process been established to document and track changes to the application?										
Does a procedure exist to ensure that management considers the potential impact to other applications or systems before initiating any changes to the application?										
Has a separate process been established for emergency changes to the application?										

Conclusion for this Section (Include All Weaknesses Identified)

Risk Category: Internal Control Monitoring										
Description/Purpose: to evaluate the protection and achievement of IT objectives, operations, laws, and regulations through defining a systems of controls, monitoring and reporting on internal control effectiveness, and documenting and responding to exceptions.										
COBIT Reference: ME-2										
Does management have a process to record control exceptions or violations?										
Has management obtained assurance of internal controls for the application through independent external/internal audit parties?										
Does management review the internal controls of external service providers, who use the application, through TPSO audits or other means?										
Does management take corrective action based on weaknesses identified in the internal control assessments for the application?										

Conclusion for this Section (Include All Weaknesses Identified)

(a) When possible, obtain applicable documentation and/or flowcharts for your future needs/requirements.

(b) Please explain in the Description/Comments column.

(1)	(2)	(3)				(4)			(5)	(6)
Optimal Internal Controls	Agency, Division/Office and Staff (Non-DIT) Responsible for IT Process and Related Controls identify the activity and business owner responsible for each IT process (e.g., agency, division, office and/or staff)	Internal Control Existence (a)				Performance Effectiveness			Description/Comments (this column must be completed) description of controls, activities, formal policies, procedures, and practices that represent internal controls related to the IT process and whether alternative or compensating controls and plans and time frames exist for addressing deficiencies	Monitoring (this column must be completed) description of activities performed to ensure controls in place are working
		Documented	Not Documented	No Control in Place	Not Applicable (b)	Satisfactory	Ineffective/Inefficient	Not Applicable		
Risk Category: Service Level Agreements										
Description/Purpose: to evaluate the controls ensuring definition and management of service levels in line with business objectives through formal procedures, review and communication, and continuous monitoring.										
COBIT Reference: DS-1										
Does management have formal procedures for creating service requirements, service definitions, service level agreements, operating level agreements, funding sources, etc. of service levels (the stated degree/level of performance/processes to be provided) for customers and service providers?										
If external parties administer key elements of the application, has management defined acceptable levels of service for these key elements?										
Does the operating level agreement for the application, which specifies the technical processes in terms meaningful to the provider, define and explain how service levels will be supported?										
Does management review the service level agreements related to the application for adequacy?										

Conclusion for this Section (Include All Weaknesses Identified)

Risk Category: Third Party Service Controls										
Description/Purpose: to evaluate controls over identification, classification, selection, and monitoring of application/IT service providers while ensuring adherence to agreements.										
COBIT Reference: DS-2										
Has management established procedures to identify and define all supplier services or relationships directly impacting the application?										
Has management identified application risks/threats relating to the supplier's service continuity for the application?										
Has management established a process to monitor the delivery of service from the supplier for the application?										

Conclusion for this Section (Include All Weaknesses Identified)

(a) When possible, obtain applicable documentation and/or flowcharts for your future needs/requirements.

(b) Please explain in the Description/Comments column.

(1)	(2)	(3)				(4)			(5)	(6)
Optimal Internal Controls	Agency, Division/Office and Staff (Non-DIT) Responsible for IT Process and Related Controls identify the activity and business owner responsible for each IT process (e.g., agency, division, office and/or staff)	Internal Control Existence (a)				Performance Effectiveness			Description/Comments (this column must be completed) description of controls, activities, formal policies, procedures, and practices that represent internal controls related to the IT process and whether alternative or compensating controls and plans and time frames exist for addressing deficiencies	Monitoring (this column must be completed) description of activities performed to ensure controls in place are working
		Documented	Not Documented	No Control in Place	Not Applicable (b)	Satisfactory	Ineffective/Inefficient	Not Applicable		
Risk Category: Data Management Controls										
Description/Purpose: to evaluate management controls over data including completeness, accuracy, availability, and protection through adequately defined procedures to back-up, test, store, secure, and dispose of data and information.										
COBIT Reference: DS-11										
Has management established procedures regarding labeling, data backup/copying, retrieval, security requirements, and etc., for data storage and archival for the application?										
Has management established procedures to inventory and manage onsite media related to the application such as hard copy documentation, hard/floppy/optical disks, magnetic tape, cables, etc.?										
Has management established procedures to ensure proper disposal of sensitive data and software for the application, such as shredding, disk erasure, file wipe, etc.?										
Has management implemented increased security, physical access controls and logical controls, for any sensitive data associated with the application?										
Conclusion for this Section (Include All Weaknesses Identified)										
Risk Category: Business Continuity / Disaster Recovery										
Description/Purpose: to evaluate controls designed to minimize interruption or loss of application/IT services of critical and key business functions through management's training of personnel, contingency planning, storing critical back-ups, and testing of contingency/recovery plans.										
COBIT Reference: DS-4										
Does management have a plan to address requirements for resiliency, alternative processing, recovery capability, etc. for the application's critical services in the event the application is disrupted?										
Has management established a framework for application continuity that is consistent with the department's business continuity?										
Has management given the critical application's resources priority in the continuity plan?										
Does management have a process to regularly update the application's continuity plan?										
Does management regularly test the application's continuity plan?										

(a) When possible, obtain applicable documentation and/or flowcharts for your future needs/requirements.

(b) Please explain in the Description/Comments column.

(1)	(2)	(3)				(4)			(5)	(6)
Optimal Internal Controls	Agency, Division/Office and Staff (Non-DIT) Responsible for IT Process and Related Controls identify the activity and business owner responsible for each IT process (e.g., agency, division, office and/or staff)	Internal Control Existence (a)				Performance Effectiveness			Description/Comments (this column must be completed) description of controls, activities, formal policies, procedures, and practices that represent internal controls related to the IT process and whether alternative or compensating controls and plans and time frames exist for addressing deficiencies	Monitoring (this column must be completed) description of activities performed to ensure controls in place are working
		Documented	Not Documented	No Control in Place	Not Applicable (b)	Satisfactory	Ineffective/Inefficient	Not Applicable		
Do personnel receive regular training for their roles and responsibilities with the application's continuity?										
Does management secure the application's continuity plans and distribute them to appropriate users?										
Does management securely store all critical backup media needed for the application's recovery and business continuity offsite?										

Conclusion for this Section (Include All Weaknesses Identified)

Overall Conclusion of Strengths and Weaknesses

I certify that this evaluation of the *Application Controls* of the internal control structure for the application defined as (_____), in effect during the two-year period ended 9/30/____ has been conducted in a reasonable and prudent manner, and I concur with the conclusions documented as a result of this evaluation, unless otherwise indicated below.

Material Weaknesses Identified: _____ Yes _____ No (If yes, attach to this letter a list of material weaknesses identified.)

Activity Level Manager Signature _____ Date _____

(a) When possible, obtain applicable documentation and/or flowcharts for your future needs/requirements.

(b) Please explain in the Description/Comments column.